Professional Perspective

How to Ensure Better Contracts with Alternative Data Providers

George Danenhauer, Raji Kochhar & Boris Liberman, Lowenstein Sandler

Bloomberg Law

How to Ensure Better Contracts with Alternative Data Providers

Contributed by George Danenhauer, Raji Kochhar & Boris Liberman, Lowenstein Sandler

July 2022

By market estimates, the global market for alternative data is expected to reach $13.91 billion by 2026, a 77% increase from $3.23 billion in 2022. Hedge funds and other trading firms hungry for any possible edge are driving the demand.

The Securities and Exchange Commission (SEC) has taken notice. Over the last few years, the SEC's top examination priorities have begun to include the use of alternative data, which is generally defined as information not contained in company filings, press releases, analyst reports, or other traditional information sources. This information can range from credit card transactions to app downloads to corporate jet flight patterns but may contain material nonpublic information, also referred to as MNPI. In a risk warning issued in April 2022, the SEC faulted investment advisers for inconsistent or weak due diligence on alternative data service providers, among other concerns.

The SEC has done more than just talk. On September 14, 2021, it brought its first enforcement action against an alternative data provider. The SEC alleged that App Annie Inc. (now data.ai), which sells data relating to mobile apps, used deceptive practices and made material misrepresentations about how it obtained its data. The enforcement action has since spurred other data providers to review their compliance policies and procedures.

Given the growing use of alternative data and the SEC's focus on this area, investment advisers need to negotiate appropriately protective contractual terms with their alternative data providers. In our experience as counsel to investment advisers negotiating and reviewing hundreds of these agreements, here are the most common ways counsel can help their clients in negotiations with alternative data vendors.

1. **Push hard for representations and warranties around the data's provenance.** Among the most significant risks of using alternative data are misappropriation claims—i.e., that a trader used data obtained in violation of law or rights of a third party—which can lead to claims of improper procedures and controls, or worst case, insider trading allegations. That's why receiving a clean bill of health on the data's origin and chain of custody is so important.

   While indemnity for third-party intellectual property claims is a relatively standard compromise provision in many licensing arrangements, it can be inadequate in data licensing, and representations and warranties around data provenance are preferable. Of course, violations of such representations and warranties should also include the possibility of meaningful damages.

2. **Require notice of any adverse event concerning the data.** The SEC has consistently emphasized the importance of due diligence around alternative data. Such due diligence is not any less critical after an investment adviser signs a contract with a data provider. Investment advisers should therefor take the opportunity in contract negotiations to seek an affirmative commitment by vendors to notify them of significant adverse events around the data for the contract's term.

   Those events could include any material breach of representations and warranties, governmental investigations, third-party claims, or cease and desist letters. The investment adviser should, in all events, be able to pause its use of the data while performing any further necessary diligence.

3. **Pay close attention to contracts with international vendors or data gathered internationally.** Representations and warranties should be reviewed considering the local jurisdiction and applicable law. Local regulations and laws, such as the EU's General Data Protection Regulation (GDPR) or China's recently enacted data security Law, could be relevant. Advisers—and their US counsel—should consult with local counsel as appropriate and as needed in the event of jurisdiction-specific concerns or novel issues.

4. **Negotiate assignment provisions**. Many data vendors ultimately want future flexibility to be acquired, so it's no surprise that assignment provisions are a frequent contract feature. As a best practice, any assignment should require notice to the investment adviser.

The notice should allow the investment adviser to confirm that the new assignee meets comparable standards reviewed during the initial due diligence of the original vendor. Consider requiring consent not to be unreasonably withheld or similar language.

5. **Beware of pitfalls with trial data evaluation agreements**. Many vendors will offer clients free weeks or months to test their data. But they won't automatically provide the same representations and warranties as for paying customers. Investment advisers should be cautious about accepting a free trial without basic representations and warranties.

   If trading personnel need to evaluate the data's effectiveness before purchasing it, they could instead ask the vendor for stale data and analyze whether the information would have been helpful. Alternatively, a trading firm could offer to pay for a limited trial with the appropriate legal protections around the data.

6. **Be mindful of auto-renewals.** Automatic renewals can be a convenient feature, especially if the contract is month-to-month. But data contracts often last a year, and renewals can sneak up quickly and take away an opportunity for fresh due diligence on the provider. Trading firms should seek an adequate notice period before the renewal kicks in, during which they may refresh their diligence on the vendor or terminate the contract.

7. **Protect against the risk that a counterparty may cease doing business—or cease engaging in the data business.** While there are plenty of established businesses in the alternative data ecosystem, startups lacking proven track records are also common. Investment advisers concerned about a potential business failure by their vendor may want to spread payments throughout a contract rather than paying a lump sum upfront. Given Covid-19 and other geopolitical risks, early termination rights and quarterly or monthly payments may be appropriate to insist upon.

8. **Value the importance of certain early termination rights.** Seek an early termination right in the event of any material diminishment in the data. For example, a service or app may see the number of unique monthly users cut in half, making the data less useful. This could occur due to privacy changes by an app store, among other reasons. Insert an early termination right if the data vendor wishes to switch to another similar underlying data provider. Among other concerns, such a switch would likely require a due diligence refresh before moving forward with the data.

9. **Beware of granting broad on-site audit rights with access to physical premises or electronic systems.** Among other issues, such rights may run afoul of other policies and procedures, including information security policies. This is another relatively standard example of an intellectual property licensing provision that does not work well for the investment management industry.

10. **Ensure the protection of confidential information.** The purchased data is not the only information that should get attention. An investment firm should be mindful that it may be providing valuable information, such as its trading positions, to the data vendor. That information should be protected. At the same time, be aware of provisions that allow the data vendor to create new data sets based on the adviser's information or usage patterns of the vendor's data.

    At a minimum, any such information should be aggregated—i.e., such that the customer represents less than a certain percentage of the dataset—and anonymized before dissemination to any third parties. If the vendor insists on rights to create new data sets based on an investment adviser's information or usage data, inquire whether the data vendor actively sells such data to third parties or includes such provisions for internal use or speculative future use.